



# Roosevelt University

## Password Policy

### **Policy 7.5**

Responsible Executive: VP for  
Technology & CIO

Originally Issued: May 25, 2006

Revised: October 15, 2008

Effective date: May 25, 2006

---

### ***Reason for Policy***

Passwords are an important aspect of digital security. They are the front line of protection for user accounts. A poorly chosen password may result in the compromising of network resources. As such, all users, faculty and staff, including adjuncts and part-time employees, are responsible for taking the appropriate precautions outlined in this policy to select and secure their passwords.

The purpose of this policy is to establish rules for the creation of passwords, the protection of those passwords, and the frequency of change.

---

### ***Entities Affected by this Policy***

The scope of this policy includes all personnel who have access to any RU information system, or are responsible for any computer account (or any form of access that supports or requires a password) on any RU system.

---

### ***Policy Statement***

#### A. Password Characteristics

1. Passwords must be at least eight characters in length.
2. Passwords must contain at least one letter, one number and one special character, e.g., !, @, (, \$.

#### B. Changing Passwords

1. When receiving a new account, the user is given a temporary password. All temporary passwords are to be changed upon the initial login after receiving a computer account. The initial login must occur within 7 days after receiving the account or the account will be deleted.
2. After the initial login, passwords must be changed at least every 6 months.
3. In order to curtail attempts to gain illicit access to an account, an account will be suspended after six unsuccessful logon attempts.
4. Previous passwords may not be reused for one year.

#### C. Password Protection

1. Passwords may not be inserted into email messages or other forms of clear text electronic communication.

2. Passwords should not normally be shared with others. If a password is shared with IT support personnel for troubleshooting, then the password must be changed as soon as possible.
3. Passwords may never be written down or stored off-line in an unsecured manner or on-line in clear text.
4. Passwords are not to be shared with anyone except for a supervisor who may require access to an account for legitimate office business. All passwords are to be treated as sensitive, confidential information.
5. Passwords are not to be revealed over the phone to ANYONE, including computer support personnel. Support personnel must never initiate a call requesting a password.
6. A password may not be revealed in an unencrypted email message.
7. Other password protection hints include:
  - a. do not talk about a password in front of others,
  - b. do not hint at the format of a password (ex. "my pet's name"),
  - c. do not share a password with family members, and
  - d. do not reveal a password to co-workers while on vacation.

#### D. Compromised Passwords

If a password holder believes an account or password has been compromised, she or he must report the incident to the appropriate system administrators and the Technology HelpDesk (312.341.6460 or [helpdesk@roosevelt.edu](mailto:helpdesk@roosevelt.edu)).

#### E. Enforcement

Any personnel found to have violated this policy may be subject to disciplinary action and loss of access to RU resources as described in the Roosevelt University Computer and Network Usage Policy.

#### F. Password Resets

Password resets may only be performed by authorized personnel (e.g., Help Desk personnel, System Administrators). To avoid fraudulent requests for password resets, certain verification steps will be taken by the Technology helpdesk including a phone call to the appropriate user, confirming request for a reset of his or her password. Technology Help Desk personnel may determine the identity of user through personal knowledge of the individual, including visual recognition, voice recognition, etc.

---

### ***Web Address***

---

To be completed by the President's Chief of Staff.

---

### ***Related Documents***

---

Policy on the Acceptable Use of Electronic Resources

---

### ***Implementation***

---

The Vice President for Technology and Chief Information Officer will develop procedures to implement this policy.